DOCID: 3189576

~~TOP SECRET~~

DF-111
(remod 1)

ARMY SECURITY AGENCY

53/49/TOSEC-AS-34-B

Copy No. 3

From: C3C/AS-34-B

To: AS-30 - AS-53 file

S-3035

S-3035 Encl. #4 1

Rec'd - 7 July 1949

RECORD COPY
DO NOT DESTROY OR MUTILATE

Declassified by NSA 08-01-2007
pursuant to E.O. 12958, as
amended, FOIA Case# 9329

~~TOP SECRET~~

DOCID: 3189576

TOP SECRET

DF-111 (revised) 53/49/TOPSEC/AS-34-B

COMMENTS ON VARIOUS CRYPTOLOGIC MATTERS

BY

ADOLF PASCHKE

The attached paper is a re-translation of material formerly issued by TICOM, ASA as DF-111, DF-111-A, and DF-111-B. With the issue of the present translation (DF-111 revised) the former translations are rescinded and it is requested that these documents be destroyed upon receipt of the present translation.

June 1949 30 pages, Copy No._____

Distribution: Normal 30 copies.

S-3035 74 1

TOP SECRET

DOCID: 3189576

TABLE OF CONTENTS

		Page
INTRODUCTION		1
I.	PERSONAL HISTORY	2
II.	CRYPTOGRAPHIC SYSTEMS OF THE SOVIET UNION	4
III.	SUPPLEMENT TO CRYPTOGRAPHIC SYSTEMS OF THE SOVIET UNION	12
IV.	ANSWERS TO QUESTIONS ON SOVIET CRYPTOGRAPHIC SYSTEMS	16
V.	CRYPTOGRAPHY OF THE CZARIST FOREIGN MINISTRY	19
VI.	RELATION BETWEEN THE CRYPTANALYTIC SECTION OF THE FOREIGN OFFICE AND OKW/Chi	20
VII.	THE FORSCHUNGSAMT OF THE GERMAN AIR MINISTRY	24
VIII.	SOME CRYPTANALYSTS IN THE FOREIGN OFFICE	26

DOCID: 3189576

INTRODUCTION

The following chapters comprise a series of reports written during 1948 by the former German Oberregierungsrat ADOLF PASCHKE, the last head of the German Foreign Office Cryptanalytic Section. During this period Herr PASCHKE was employed as violinist in the Marburg orchestra and resided at - Ockerhaeuser Allee 35, Marburg/Lahn.

The first three chapters (GENERAL HISTORY, CRYPTOGRAPHIC SYSTEMS OF THE SOVIET UNION, and SUPPLEMENT TO CRYPTOGRAPHIC SYSTEMS OF THE SOVIET UNION) were voluntarily submitted in January 1948 by Herr PASCHKE to the United States Security and Liaison Officer in Wiesbaden, Germany and passed by the officer through ASA Europe to Army Security Agency.

Chapters IV through VIII are Herr PASCHKE's answers written in June 1948 to specific questions asked by Army Security Agency through its representative in Europe. In Chapter IV the specific questions have been retained at the beginning of the section. This has not been thought necessary for Chapters V through VIII.

In September 1948 Herr PASCHKE verbally expressed to the ASA representative in Europe his desire to write a historical study of cryptography and cryptanalysis during World Wars I and II. This he was willing to do for a remuneration which would enable him to devote his time to the work. No such project was contemplated by Army Security Agency and Herr PASCHKE was so informed. No further reports have been received by this Agency from Herr PASCHKE.

DOCID: 3189576

CHAPTER I. PERSONAL HISTORY

I was born 20 September 1891 in St. Petersburg, Russia, as the son of German parents.

In St. Petersburg I attended the Schubert Preparatory School and the Gymnasium of the German St. Petri-School. After graduation in 1909 I studied law and national economics in Berlin and St. Petersburg and concluded my course of study with the first law examination which I took in 1914 at the University of St. Petersburg.

In the First World War I was for ten months a civilian internee in Russia, was exchanged, and came to Germany there in the autumn of 1915 I was posted to the Signal Corps and was employed there in the cryptanalytic service. Cryptanalysis was at that time an entirely new field in Germany. I had opportunity to study in detail the results achieved in the first year of the war; was trained according to the cryptographic standards of that time, and then worked successfully in the cryptanalytic service on the eastern front until 1918 and achieved numerous first solutions. I was also trained in radio work and became a Reserve Lieutenant in the Signal Corps. In the fall of 1918 I was transferred to the Chief of Signal Communications in the Grand Headquarters, where I was able to expand my knowledge in the realm of cryptanalysis.

After the end of the war I was summoned in 1919 to the German Foreign Office as an expert in cryptography. I worked there in a leading position until 1945 on the extension of the art of cryptography, especially on working methods. The scientific discoveries in the realm of cryptography went forward with great strides in Germany during this period. I, myself, made a number of these advances. Through my work I knew the cryptographic systems of all the nations of the world as of 1945. I worked with particular intensity on the cryptographic systems of the Soviet Union, the Border States, Austria, the Vatican, Italy, Greece, France, and Czechoslovakia.

In 1927 I became Regierungsrat, in 1939 Oberregierungsrat, and in 1941 I was charged with the direction of the current cryptanalytic service in the Foreign Office.

DOCID: 3189576

I am complete master of the Russian language both written and spoken; I have school knowledge of French and English, and some knowledge of Italian..

In May 1945 I was taken from my place of evacuation in central Germany (Burgsheidungen) as scientific expert in my field with 23 colleagues and co-workers "for information purposes" to London and from there in June 1945 to Marburg where until January 1946 I was at the disposal of the Military Government. In this period I was briefly questioned approximately five times on my previous work.

I am at present employed in Marburg as an orchestral musician (violin).

In denazification proceedings I was placed after the first hearing in Category V, "exonerated" (Entlasteten), after the second hearing I was placed in Category IV, "fellow traveller" (Mitläufer). The latter finding is correct.

Since 1920 I have been married to Adele, the youngest daughter of the Evangelical University-theologian, Prof. Dr. D. Carl Cornill; I have two children, a 20-year old daughter, who is studying medicine in Marburg, and a 12-year old son, who is attending the Gymnasium.

DOCID: 3189576

CHAPTER II. CRYPTOGRAPHIC SYSTEM OF THE SOVIET UNION

Preface

The present account has been prepared from memory without any written notes. Yet it should not contain any errors of fact, only the dates are not always certain.

This account will describe in general outline the course of development of cryptographic thought in the Soviet Union (SU), will present the basic outline of the cryptographic system employed at present, will indicate the problem of possibility of solution of this system in its essential point, and finally will point a way by which an evaluation of the telegraphic material of the SU is possible even without decipherment.

Everything in this account applies to the period up to May 1945. Since then I have had no opportunity to work on the matters treated here.

The Development of Cryptography in the SU

In the course of 13 years from 1918 to 1930 the cryptographic systems of the SU have developed from primitive beginnings to systems which in respect to their security against unauthorized decipherment belong to the best systems of the present time. There have been no essential changes since about 1931.

In the first three years, from 1918 to 1921, one could note in the Soviet cipher system the conspiratorial experience of their inventors. In those years systems were employed whose key either could be kept in the head without any written record or which were not to be recognized from their outward appearance as cipher material.

At this time the main system was "simple" (not double) transposition. It was first used only in the most primitive form, merely joined with transcription into the Latin alphabet; later it was complicated by the use of conversion tables. At the end of this development, transposed 3-digit codes appeared whose size, however, was considerably less than 1000 groups. The transposition keys were divided according to the well-known method from proverbs, quotations, passages of poetry, etc. In addition to the transposition system, 2-digit conversion tables were also

DOCID: 3189576

used as independent ciphers; those were reenciphered in various fashions, of slight effectiveness.

At that time it was learned from a deciphered telegram from Moscow that the solubility of simple transposition systems had been proved by the experts in Moscow. Perhaps one of the cryptographic experts of the former Czarist Foreign Ministry, who had been engaged for this work by the S. U., gave this information. The Czarist cryptographic service had a long tradition behind it and stood on a high plane.

Sometime around 1922 the transposition system was abandoned, without making any attempt at double transposition. A period of experimentation followed. Various systems were used in which it was impossible to identify any common principle. One of them had a striking resemblance to one of the best cryptographic systems of the Czarist Foreign Ministry: a 3-digit code was periodically reenciphered with thirty 1-digit conversion tables which were assembled according to daily keys.

About 1923 a basic change of cryptographic system appeared. Larger codes were introduced of which some had code groups of varying length (2, 3, and 4-digit groups); while others were composed of 4-digit groups. These codes were reenciphered by digit sequences which were read off from number tables having a size of 5000 digits (1000 5-digit groups in 100 rows of 10 groups each). Reencipherment was carried out by a system of addition. The size of the number tables was doubled through being read off in a serpentine fashion: by row from left to right, right to left, left to right etc., so that each row - according to the starting point - could be read off from left to right as well as from right to left. The reading off could begin with any group, so that there were 1000 possible starting points. Each diplomatic mission in foreign countries had its own table for telegrams to and from Moscow; in addition there were a special table for telegrams between diplomatic representatives in foreign countries, and for circular telegrams, and a special table for the telegrams of the Comintern. The period of use of these tables was four to eight weeks. The enciphered digit text was changed into letter cipher text by a conversion table (two digits = two letters).

DOCID: 3189576

The ciphers described above were systems used by the Peoples Commissariat for Foreign Affairs; yet, in the first years of the Soviet regime the telegrams of other Commissariats and the foreign telegrams of the Comintern were also enciphered with them. In the course of time each Commissariat received its own ciphers. The Comintern, it is true, received, in addition, special ciphers which consisted of cover names and small conversion tables with which only individual words of the telegram were enciphered; these ciphers were ostensibly designed only as a security measure in the internal operations of the service. These partially enciphered telegrams of the Comintern were handled as clear text by the cryptographic bureaus of the Foreign Commissariat and the diplomatic missions in foreign countries and were enciphered once more with their respective cryptographic systems.

After solution of the reenciphorment table and of the code had been effected, one did not obtain clear text from these Comintern telegrams but rather a text in which all proper names, countries, and cities were replaced by cover names or cover words and for which it was necessary to solve the conversion tables with which text material intended to be kept secret, for which there were no cover words, had been enciphered. While solution of the conversion table gave no trouble, the interpretation of the cover names and cover words was difficult, the more so since the cover names differed according to countries. So, for example, the word "London" in Berlin traffic was given a different cover name from that used in Paris traffic.

Although the progress in the development of cryptographic systems in the SU from 1918 to 1923 can be designated as notable, yet the systems were always solvable. Moreover they were solved. They were also solved in England where in 1927 a White Paper was published in which some deciphered Soviet telegrams were contained which revealed the policy of the SU with respect to England. This publication had the result that soon afterwards the Soviet cryptographic systems were changed and their solution became extraordinarily difficult.

The SU now introduced the so-called "Pad System" (Blockverfahren). A number of sheets were bound together into a pad, on each of these sheets either 275 or 550 digits were printed in 5-digit groups in 11 rows. Each pad page was intended for a single telegram. The pads with 275 digits to the page were intended for the reenciphement by addition of code text up to 500 digits in length, the pads with 550 digits to the page were intended for code texts with a length of from 551 to 1100 digits; code texts with a length greater than 1100 digits had to be reenciphered in parts, each part with a different pad page. The digit sequence on a pad page was, as in previous systems, read off in serpentine fashion (left-right, right-left, left-right, etc.) and was used twice at most in the same telegram because of the limitation of length of text to 550 or 1100 digits as the case might be. For the second use the digit sequence was read off in the reverse direction: all rows which formerly had been read off from left to right were now read off right to left and conversely. Each pad was printed in only two copies, one copy for the sender to encipher with -- by addition, the other for the receiver to decipher with -- by subtraction. The final reencipherment with a conversion table for changing the finished digit cipher text to letter cipher text remained in use. This two-place table was later replaced by a single place table (1 digit = 1 letter) which remains unchanged up to the present.

The cryptographic regulations were almost always strictly observed by the cryptographers. Only rarely did telegrams appear which, contrary to regulations, were longer than 1100 digits, and in which a pad page had been used more than twice. So long as the codes used were known, due to the solution of earlier systems, such telegrams enciphered contrary to regulations could be more or less completely deciphered. The telegrams enciphered according to regulations, on the contrary, could now be solved only in fragments, if at all.

Circular telegrams were no longer sent in circular systems used up till now but a circular telegram for "n" missions was enciphered "n"-times with the pad of the individual missions. For telegraphic communication between diplomatic missions in foreign countries the previous system with

DOCID: 3189576

digit tables remained in use for some time. The length of these tables was doubled however (to 10,000 digits). Later these table systems were given up entirely so that telegrams between the diplomatic missions now had to be passed over the Moscow Central, unless a special pad had been printed for communication between the two diplomatic missions, which was rarely the case.

The Cryptographic Systems in Use at Present

About 1930 the last step in the perfection of Soviet cryptographic systems was taken. It was introduced for the encipherment of code text by means of pads with digit sequences 275 digits long; a pad usually contained 35 pages. Each pad sheet was now used only a single time and was read from left to right. A second use within a message of a digit sequence by reading off in inverse fashion was discontinued, as was the reading off in serpentine lines. The maximum length of telegrams was abolished. For each telegram as many consecutive pad pages were used as the length of the telegram required. Each page of a pad was considered "used up" when used once and, according to regulations, was destroyed immediately thereafter. The use of a single place conversion table for changing the digit cipher text into letter cipher text continued.

The above description of cryptographic systems which have been used since 1927 concerns the systems of the Peoples Commissariat for Foreign Affairs. The systems of the other Commissariats are likewise - for foreign communications - based on the pad system and can be distinguished from the first and from one another only by non-essential details, e. g., by the length of the digit sequence on a pad page or by the number of pages in a pad. Each Commissariat has its own code. These codes are usually alphabetically compiled so that a single volume may be used for enciphering and deciphering.

The cryptographic systems of the Comintern for its signal communications with the Communist parties in foreign countries again form an exception; since 1930 they have been constructed according to another system. The cryptographic service of the SU probably did not wish to expose its

DOCID: 3189576

cryptographic systems to the danger of falling into the hand of the police of other countries as the result of a house-search. Therefore cryptographic systems were developed for the Comintern, where the most essential parts, that is, the keys for the encipherment - were not outwardly to be recognized as cryptographic material. Alphabetically constructed digit codes were enciphered with the aid of book text which was converted to digit sequences by an easily memorized conversion table. A particular instance deserves mention: it concerns telegraphic material of a total length of about two million digits. In the course of the work of solution it was established that it had been enciphered by means of five books which gave an encipherment sequence of about five million digits. An apparently hopeless case. And yet solution was achieved. It was made possible by the far more frequent use of individual passages in these five books than would be expected by the laws of probability, a psychologically explicable phenomenon; one of the books was used much more often than the other four, for some insignificant reason or other; the right-hand pages were used several times as often as the left-hand pages because of convenience: the pages in the middle of the book were preferred; the first and second sentences on the page selected were especially favored as the starting point for the enciphering sequence. Thus some if not any very great amount of material emerged with the same encipherment. This amount of material was enough for solution.

The Question of the Possibility of Solving the Cryptographic System Employed at Present

The problem of solving the modern system of the SU (excepting the system of the Comintern, the reappearance of which is uncertain) depends on the question of how many copies of each pad page are printed. Up to the present it has never been possible to give an unequivocal answer to this question. To clarify this question I carried out sometime in 1930 a thorough and minute study of the pads of the Peoples Commissariat for Foreign Trade. In the course of this investigation pad pages were found which appeared

three times in different pads at considerable intervals of time and quite irregularly; these pad pages must have been printed in six copies. Unfortunately in this investigation I started with the false promise that the reappearance of a pad page was to be expected only on one and the same traffic circuit so that a great amount of material available at that time from other traffic circuits remained unexamined. The results of this investigation cannot therefore be taken as conclusive and one must count on a much greater number of copies of the same pad pages, at least at that time.

How many copies of pad pages are printed at present cannot be established without thoroughgoing investigation. It is already known that the number of copies of a pad page cannot be fundamentally very great since these pages, at least in the Red Army during the war, were prepared on the typewriter - with carbon copies. The possibility must also be reckoned with that the pad pages are at present made only in two copies and for a single use.

It may still be worth while to examine the question whether, in spite of perhaps small chance of finding a sufficient number of the same pad pages to make decipherment possible, a very urgent effort in this direction should not be undertaken. Without having the results of such an investigation at hand, one can neither deny nor affirm the possibility of solving the cryptographic systems of the SU.

Everything stated above holds good only for normal circumstances, that is, when the cryptographic service of the SU can currently prepare adequate cryptographic material (pads) for the very extensive telegraphic communications and distribute them to the representatives in foreign countries. In very exceptional circumstances it can happen that it is impossible to prepare and distribute cryptographic materials as required. Then it is impossible to prevent the emergency practice of reusing pads several times. This actually occurred in the Red Army several times during the last war and made possible the decipherment of the telegrams concerned.

DOCID: 3189576

The Possibility of Evaluating the Telegraphic Traffic of the SU without Decipherment

The telegraphic traffic of the SU can also be evaluated in a special fashion without decipherment: between the Foreign Office in Moscow and its foreign representatives pass not only the telegrams of this ministry, of ambassadors and consulates abroad but also with the same address - not outwardly recognizable - telegrams of the military intelligence service, of the Ministry of the Interior (formerly GPU) and probably of the liaison sections of the Communist party. These various types of material can be recognized and separated by solution of the so-called indicator groups [Kenngruppen] which occur in each telegram (reenciphered and not easily discoverable). Solution of the indicator groups and their current decipherment make possible the noting of the different originators and recipients. Such a notation by time and place gives clues respecting the shifting activity of the Soviet government in foreign politics, in the realm of internal politics, and in the field of military intelligence. Such a notation also gives hints about the organization of these services in foreign countries. Any fear of an intentional deception through fictitious telgrams to provoke false conclusions is without foundation since the indicator groups are considered secret. On the contrary, by a current decipherment of the indicator groups any attempts at deception through increased flow of messages can be easily recognized as such.

DOCID: 3189576

CHAPTER III. SUPPLEMENT TO CRYPTOGRAPHIC SYSTEMS OF THE SOVIET UNION

Supplementing points III and IV of my previous report on "Cryptographic System of the Soviet Union" I should like to present the following in order to make clear the course of my cryptanalytic work on the modern Soviet Russian cipher system and so to explain why I have given up my former pessimistic attitude regarding the possibility of solving those systems and now take a more optimistic view.

In the interval following the publication of the English White Paper, which gave occasion for changing the Soviet Russian cipher system, and preceding the introduction of the new system, a few telegrams were sent which had been enciphered by the old system and could be deciphered. From the content of these messages it was evident that at that time the Russians did not reckon with the solution of their cipher systems by scientific methods but rather with the successful betrayal of their cryptographic material. The NKID gave its foreign representatives strict instructions to destroy at once all cryptographic material not needed for current telegraphic traffic in order to render any further betrayal more difficult. Hence it may be assumed that in creating the new system the aim was to create a system that would be secure against treachery. The additive pad system which was introduced shortly afterward did actually afford ideal security against treachery: used pad sheets could and had to be destroyed immediately after use; the pad sheets which had not been used were protected against treachery to a considerable degree by binding in sealed pads.

Soon after the introduction of the new cryptographic system I succeeded in making a few significant discoveries, including the recognition of the double use of additive sequences in all telegrams which were longer than these sequences, and to be sure following the previous method of taking off the additive - first from left to right, and the second time from right to left. On the basis of my observations I diagnosed the presence of the pad system. This diagnosis was later proved correct by captured material.

Nevertheless, I did not think my diagnosis could be upheld unconditionally because of various new observations.

I soon established that, quite unexpectedly, many pad sheets occured twice and even three times at completely irregular intervals. This observation raised doubt in my mind as to the correctness of my diagnosis of the presence of a pad system. The production of a considerable number of identical pad sheets seem to me to be absurd, since it signified no essential facilitation or shortening of the mechanical production of pad pages, which I assumed to be used. In the case of the German and Czechoslovak pad systems known to me the sheets were quite logically produced in only two copies, i. e., for a single use. Therefore I thought it necessary to reckon with the presence of some other system, possibly with the use of rather large books with number sequences, the use of which for encipherment (as I assumed) was controlled by the central office by the issue of use-keys which would to some extent "prohibit" the use of these additive sequences within the frequency limits assumed to be admissible. As I saw it, the problem to be solved was how many repetitions, possibly with different methods of taking out the additive, this "retaining" of use, which was centrally controlled and removed from the dangerous option of code clerks, permitted.

Starting with this idea which was based on my experience with earlier Russian cryptographic systems, I now carried out an extensive study endeavoring to find at other positions in the traffic those portions of the additive sequences which I had solved. In my study I, however, never found more than three repetitions. Moreover, these repetitions always included the entire additive sequence of a telegram and always were taken out in the same fashion. Unfortunately in this study I started with the false assumption that the repetitions could only occur on the same circuit, since the Russians had hitherto issued special cryptographic material for each individual circuit (aside from circular and ring system). Therefore I failed to include in my study all traffic available to me from different circuits. Therefore the result of my study at that time cannot be regarded

DOCID: 3189576

as exhaustive. Probably it is necessary to reckon with a larger number of repetitions of identical pad pages.

About 1935 I broke off intensive work on Soviet Russian systems because I had to devote myself to other important work. Since then I have merely had the Russian system observed in order to note any changes and I have limited myself to the evaluation of the indicator groups (Kenngruppen).

In 1941 I found my first diagnosis of an additive pad system completely confirmed by captured material; my later doubts as to the accuracy of this diagnosis were dispelled. However, other tasks which fully occupied my time left me no opportunity to combine the information gained from the captured material with the results of my earlier studies. Released from my previous labors I have during the past few years gone over what I then neglected and have carefully thought through all details known to me from my previous study. As a result I have come to the conclusion that - rebus sic stantibus - one must reckon with the possibility, that the Russians even now are preparing a relatively large number of identical pad pages which are bound in completely irregular sequence in the pads.

The following considerations favor this assumption: in the cipher regulations which I had found in the captured material was a provision that the name of the recipient and the sender of the message, as well as the actual date of the telegram (not the transmission date, which stands in clear digits at the end of the message) are to be inserted in the middle of the message text. This cryptographic habit of the Russians was already known to me from my decipherment. It can only be intended to avoid characteristic message beginnings and endings and thereby to render solution more difficult. How rendering solution more difficult in the case of an absolutely unbreakable system would be such a senseless procedure that I really should not expect it to be adopted by the highly qualified cryptographic experts of the Soviet Union.

Moreover, the Russian predeliction for codes with groups of varying length, i. e., for codes consisting of 4- and 5-digit groups, for instance, might be explained by the desire to render solution more difficult. Such codes do render the solution of the encipherment much more difficult, on

DOCID: 3189576

the other hand, they are very unhandy for one's own code clerks. Finally the conversion of the digits of the completed cipher texts into letters might have the same purpose of rendering solution more difficult, since in this way the use of the difference method, the classical method of solving additive decipherments, is rendered impossible as long as the substitution key employed remains unknown.

I have no illusions regarding the possibility of solving Soviet Russian systems. I am quite aware that the Russians, contrary to all logical deductions from their cryptographic habits, could at the present time be producing pad pages for one-time use so that any possibility of solution would be ruled out. However, since many things indicate the use of a considerable number of identical pad sheets, I should - if I were in a position to today - make without fail a thorough investigation covering all traffic, such an investigation never having been made anywhere at anytime, as I have previously mentioned. I have worked out the plan for such a study in all details. It would have to begin with the solution of the "indicator groups" (Kenngruppen), which would make possible the sorting of the traffic according to the various types of pads, hence with a piece of work which - as I have explained earlier - carries with it the possibility of a significant evaluation of its result for intelligence purposes. Therefore it would be of great significance in and of itself even in case the attempt to solve the system should end in failure.

Obviously I have no opportunity of making this study, since I have none of the material. It should be comprehensible that I entertain an ardent desire to make such a study, or at least to participate in it, since during 20 years of work on Russian cryptographic systems I have been able to gather information and experience and have achieved successes, such as have not been achieved by any other expert either in Germany or in any other European country. I am not acquainted with American work on these problems and its successes.

Therefore I request that the question of whether in some way or other I can be given a chance to attempt a decipherment be given careful consideration.

DOCID: 3189576

CHAPTER IV. ANSWERS TO QUESTIONS ON SOVIET CRYPTOGRAPHIC SYSTEMS.

1. You stated previously that additive pads employed by the Red Army during the war were prepared on the typewriter with carbon copies. Have you seen any of characteristics which might indicate that pads were prepared by the typewriter, such as corrections made by strike-overs, letters instead of digits, or other general typographic errors?

In 1941 I had in my hands some six additive pads of the Red Army and investigated them thoroughly. They were captured material which I had received from OKW. All the pads had the same number of sheets, 50 each, if I am not mistaken; on each sheet was the same number of 5-digit groups, 50 each, if I am not mistaken. Typographical errors (letters for digits and other mistakes) or corrections were not present in the digit groups. Probably no sheets with such errors were incorporated in the pads. However, the groups were beyond a doubt written with a typewriter. In the pads were found both original copies and carbons. In one pad, which attracted my notice particularly, originals and carbons followed one another alternately. The material available to me was not sufficient for me to make an approximate estimate of the number of copies which had been made of each sheet, basing this on the ratio of originals to carbons. Nevertheless, the number of carbons was noticeably greater than the number of originals.

That the digit groups on the pad sheets had been written on a typewriter, hence came from the head of a person via his hands and not from a printing machine which automatically formed digit groups, could be recognized by the characteristic digit sequences familiar to me from many Russian, Polish, and Italian keys which were prepared manually: e. g., a preference for the middle digits (4,5,6), the avoidance of zero in many cases, a preponderance of short intervals between successive digits, frequent repetitions of pairs of digits in a group (abcbc or abubc).

It is a very difficult task to make up many long sequences of digits out of one's head quickly without marked deviations from "probability." Such "psychological regularities" in digit sequences (and, of course, in letter sequences) not compiled by machine can, under some circumstances, materially facilitate current decipherment. From my practical experience,

DOCID: 3189576

I know several cases where such "psychological regularities" were the determining factor in decipherment.

2. Do you have any reason to believe that pads prepared by typewriter with carbon paper were a regular procedure and not a wartime expedient of the Red Army?

I do not know whether the production of additive sheets on the typewriter was a regular thing in the Red Army or an emergency measure dictated by war conditions. The pads which I saw showed a wartime emergency character; the additive groups were typed on the back of old geographic maps and the binding was very primitive.

I remember having heard quite a while ago that around 1930 in some South American country some cryptographic material of a Soviet Trade Mission was confiscated and that this material came to Washington. In this connection it would be very important to determine how this material, which almost surely consisted of pad sheets, was produced: whether printed, multigraphed, or typed on the typewriter.

3. Which ministries and organizations other than the Red Army used this type of pad?

In 1945 the additive pad system was used for encipherment by: (a) the Peoples Commissariat for Foreign Affairs and all its diplomatic and consular representatives in foreign countries, (b) the Peoples Commissariat for Foreign Trade and all of its foreign representatives, (c) all foreign service officers of the Military Intelligence Service and the corresponding Moscow central office, (d) the GPU and all of its foreign agents insofar as they were assigned to diplomatic or consular missions. The GPU had, however, introduced the additive pad system in its foreign traffic relatively late, only in the 1940's, if I am not mistaken. Probably lengthy digit tables were used for encipherment before that time.

The Russians do not seem to use the pad system for internal traffic (with the exception of Red Army radio traffic). In the captured material which I have seen the digit sequences for encipherment of the encoded texts of internal Russian organizations were contained in relatively large printed digit tables. It is noteworthy that directions issued with these printed tables provide that used digit groups were to be crossed out and were to be used again only when the entire table had been used once.

DOCID: 3189576

4. Do you know of any caches of Russian cryptographic material or files of Russian traffic in addition to the records of your section which were at Burgscheidungen?

All of the Russian cryptographic material available in the Foreign Office in Berlin and all telegrams were destroyed in 1945. In March 1945 I personally instructed my evacuated section in Burgscheidungen, where a part of this material was cached, to destroy it entirely. I do not know whether or to what extent this instruction was carried out. Shortly before the capture of Muelhausen in Thuringia by the United States Army, a railroad freight car was dispatched from there in the direction of Munich with all of the traffic of all countries decrypted in the Foreign Office during the years 1918-1945. What became of this freight car I was not able to learn.

All the Russian material in GCH/Cbi was destroyed by fire in 1944; likewise the material in the Air Ministry Research Bureau (RLM/FA).

I do not know of any other storage places in Germany in which Russian cryptographic material and telegrams may be cached. Moreover I do not believe that there still are any such caches.

5. Was there any system of cover words or cover names which could be identified in traffic of Soviet Russia?

Concerning cover words and cover names there is not much to say. They were used in the telegrams of the GPU, of the Comintern, and of the Military Intelligence Service, but not in the telegrams of the Peoples Commissariat for Foreign Affairs and of the Peoples Commissariat for Foreign Trade. The cover words and cover names were intended as a security measure against their own people through whose hands these dispatches must go. They were not intended to make decryption more difficult; yet their correct interpretation in decrypted telegrams was often very difficult since they were constantly changed and were intended for use only within a definite small circle.

No definite system, e. g., the same initial letter for the true name and for the cover name, could be identified for either cover words or cover names. Names of persons, cities, and countries were replaced by first names, last names, or designation of occupation; amounts of money by some class of goods with designation of the amount, so, for example: "Constable" was

DOCID: 3189576

Berlin, "1000 meter" was "cable 1000 Reichsmark," "500 kg log brisble" was "500 pounds sterling." Naturally, verbs were replaced by verbs in order to preserve the sentence structure.

CHAPTER V. CRYPTOGRAPHY OF THE CZARIST FOREIGN MINISTRY

During the years 1919-1920 I worked through all of the cryptographic material of the Czarist Foreign Ministry available in the German Foreign Office. I can therefore give some account of these. Inasmuch as I have not concerned myself with this material since that time, I can give only from memory an outline, without details, based on work done so long ago.

The entire cryptographic material which I saw was obtained not by cryptanalysis but by purchase from disloyal Czarist officials.

The chief system consisted of a Russian and a French 3-digit code, each of about 1000 groups. The encoded text was enciphered with 30 single-digit conversion tables which were produced by three-digit slides. One slide was designated for the first digit of the code group; a second for the second digit; a third for the third digit. The setting of the slides was effected by keys which changed daily; these varied from code group to code group, so that 30 different single-digit conversion tables were used for the encipherment of a single telegram. Both digit sequences of the three slides were also changed frequently.

With the then status of cryptanalysis it would not have been easy to solve this main system without knowledge of the code and of the keys, since the traffic for each day was light. It must, however, be considered a solvable system since the frequencies and repetitions of the code text were preserved at a period of 30 digits. Characteristic beginnings and endings of telegrams and a large number of passages spelled out -- necessitated by the smallness of the code -- could not fail to furnish adequate possibilities of making a correct diagnosis of the system and achieving the solution of a number of daily keys. Solution of the small code would then have been easy. I have no practical experience in the decipherment of this system. I do not know whether it was solved in any country. But probably it was not necessary to solve the system since it was possible to buy

DOCID: 3189576

In addition to this main system the Czarist Foreign Ministry used a larger digit code with the designation "Kama," which - if I am not mistaken - was alphabetical and was used in most cases unenciphered for reports of very little secrecy. After 1917 it was still used for a short time by the Czarist "Emigre" diplomats - according to my recollection - likewise without encipherment.

I learned from a Russian cryptographic expert, Nikolai Novopaschenny,j who worked in OKW/Chi, that the Czarist Foreign Ministry also frequently used digit sequences for additive reencipherment, which were intended for one-time use. They were of varying length but could never be a multiple of the number of digits of the code group, but could be used more than once in a telegram. I did not find such telegrams and such keys in the materials.

It is noteworthy that in spite of the relatively high state of cryptography of the Czarist Foreign Ministry the cipher systems of the Czarist Army were downright miserable. The complete decryption of the radiograms of the Russian Army during the World War of 1914-1918 by the German cryptanalytic service gave the German Army Command constantly and uninterruptedly a perfectly clear picture of the disposition and of the movements of the Russian troops and, consequently, of the intentions of the Russian High Command; this made a decisive contribution to the German victories.

The cryptanalytic service of the Czarist Foreign Ministry, according to everything I have heard and read, must have been exceptionally good.

CHAPTER VI. RELATION BETWEEN THE CRYPTANALYTIC SECTION OF THE FOREIGN OFFICE AND OKW/Chi.

The Cryptanalytic Section in the Foreign Office was formed at the end of 1918 by recruiting a number of experts of the former German Army and Navy who had worked successfully in cryptanalysis during the First World War. OKW/Chi (at this time known as the "Cipher Section" of the Defense Ministry) was formed later, about 1921. During the time of the Weimar Republic cooperation of the two service sections was not very intensive. They were and remained, up to their dissolution, fully separated service sections without common superintendence. Their relation to one

DOCID: 3189576

another and their cooperation were directed fundamentally by the Reich Ministers, or by their deputies. The Foreign Office had scruples about bringing to the knowledge of the Defense Ministry in a lump sum decipherments achieved in this service. Corresponding instructions to keep silence went out to all workers involved. Accordingly, I had to keep the decipherments of Soviet cipher systems secret for a long time from the Cipher Section of the Defense Ministry. The Foreign Office, however, was dependent on the radio intercept service of the Defense Ministry, since it had no intercept facilities of its own. According to the principle "Do ut des," the exchange of cryptanalytic information between the two services grew increasingly intensive. Originally, the Cipher Section of the Defense Ministry was to decipher military telegrams and the messages of the foreign Military Attaches, while the Cryptanalytic section of the Foreign Office, on the other hand, handled diplomatic and consular material. This division of labor, worked out at the green table but probably never meant seriously, was never observed by the Defense Ministry or later by the Armed Forces; instead, the Cipher Section kept expanding its work in the diplomatic field. The chief reasons were: the scanty receipts of military radiograms and probably the withholding of cryptanalytic results by the Foreign Office information which the Defense Ministry did not believe it could forego.

The intensity of cooperation between the two cryptanalytic services was also dependent on personal factors. It was for example, intensive when the Cipher Section of the Defense Ministry was headed by the then Captain, later General, Fellgiebel, who had been a regimental comrade of the Chief of the Cryptanalytic Section of the Foreign Office, Mr. Selchow. It was slowed down when the personal relations were disturbed under the successors of Captain Fellgiebel. But in spite of all checks cooperation between the two services constantly increased and received a new impulse through the accession of a part of the workers of OKW/Chi to the Research Bureau (Forschungsamt) of the German Air Ministry which was formed by them. The claim to totality often stressed by the FA and the consequent continual endangerment to the previous cryptanalytic sections caused them to make a closer alliance with one another. Practically, the cooperation of OKW/Chi

DOCID: 3189576

and the Cryptanalytic Section of the Foreign Office was as follows:

a. Supplying of radio intercepts of OKW/Chi to the Foreign Office,

b. Joint work on some new solutions,

c. Exchange of current solutions of code groups, keys and other cryptographic material,

d. Exchange of experiences.

On the other hand, deciphered messages were not exchanged.

The extent of cooperation, which was carried out mainly by the individual national desks of the two services, depended understandably - although not excusably - very much on the personal relationship between both national desks. If one group took a very domineering attitude toward the other - whether properly or improperly makes no difference - the collaboration went badly; if they esteemed each other, the exchange functioned very well to the advantage of both sides.

The results of this collaboration, considered as a whole, were important and in truth for both parties. The common human weakness of looking at one's own results with a magnifying glass while looking at the results of one's rival with a reversed spy glass, frequently led, naturally enough, to false estimates of the usefulness of this collaboration.

At the beginning of the War, I received the order to encourage to the utmost our collaboration with OKW/Chi. I think that I carried out this assignment successfully despite all checks. In this connection my good relations with Mr. Fenner, whom I have known since my boyhood, were most useful. I myself had always been an open advocat of close cooperation between the two services. Some problems in which both services had an interest were divided and in this way duplication of effort was completely avoided. Work results of current decipherment were exchanged by the quickest possible means. Some national desks were merged in one place, as, for example, the Turkish desk in my section in Dahlem. A number of workers of OKW/Chi were assigned to my section, and some of my workers to OKW/Chi. After the working quarters of OKW/Chi were bombed out, I received a number of Mr. Fenner's workers in my offices. Finally I acted - although unofficially -

as the honest broker for the two rival brothers, OKW/Chi and FA, in regard to their work results which they did not wish to exchange directly with each other.

Considered as a whole, the quality of work of both services stood on about the same level. Some national desks were better in OKW, other in the Foreign Office, due to the different qualifications of individual workers but also to the greater allocation of personnel to some tasks. The quality of the editing of the deciphered texts was probably better in the Foreign Office since - at least before the era of Ribbentrop - its quite differently disposed circle of readers laid great stress on a painstakingly accurate and faithful reproduction and translation of the original texts, even at the expense of completeness, while the OKW circle of readers preferred a smoother and more readable text, even at the expense of accuracy.

CHAPTER VII. THE FORSCHUNGSAMT OF THE GERMAN AIR MINISTRY.

I have personal knowledge only of the cryptanalytic section of the Forschungsamt; with its other sections, e. g., the telephone monitoring service, I have had nothing to do and I have only occasionally seen some results. The following remarks refer only to the cryptanalytic section of the FA.

For the other German cryptanalytic bureaus, the FA existed as a purely party organization, in which some employees of OKW held key positions; these were men who saw in their existing work no favorable prospect for promotion, since they belonged to the "second string." This opinion is undoubtedly correct. An actual necessity for setting up a new cryptanalytic service alongside the already existing and well functioning services did not exist. If one desired to centralize the cryptanalytic services it would have been possible to unite the already existing services or to create a head organization. Career prospects may well have played a major role in the founding of the FA. "Second string" personnel, however, were not the only ones concerned; by way of justice one should note that among the leading men of the FA there were also some capable people.

DOCID: 3189576

The strength of the FA lay in its good organization which was made possible and was supported by its very great financial resources. For its well paid workers many amenities of the service were provided. Unusually quick possibilities of promotion doubtlessly spurred its workers.

Very soon after the formation of the FA a sharp conflict developed between it and OKW/Chi, mainly through completely unqualified personal attacks on the then Oberregierungsrat Fenner by his former associates who had gone over to the FA. Because of this, no collaboration whatsoever developed later between the two services.

Up to 1937 the FA worked in complete isolation from the other cryptanalytic services. In these years it reconstructed, probably from the memory of its workers who came from OKW, all of the known cryptographic material which they had not been able to bring - at least not legally - with them on their secession from OKW.

The FA had secured a monopoly on interception and it supplied the other cryptanalytic services with intercepted telegrams. OKW/Chi received from the FA only cablegrams since the right to intercept radiograms had been reserved to the Armed Forces.

In the summer of 1937 the Cryptanalytic Section of the Foreign Office received the order to take up collaboration with the FA and to put all of its cryptographic material at the disposal of the FA. Because of the known principle of totality of the FA, the Foreign Office workers were not eager to carry out this order. However, they had to comply and attempt "to make the best of it." In this connection it was revealed that up to 1937 the FA had had no noteworthy results in most of the difficult fields of work. It now received the complete results of the many years of successful work of the Cryptanalytic Section of the Foreign Office. The collaboration now set up revealed that there were a few talented young workers in the FA who, properly trained, could produce good work. The quality of work of the FA improved in the course of the years and finally reached a relatively high standard. We utilized the great personnel strength of the FA for the furtherance of tasks of special interest to us, by turning over to the FA the work which was too great for our lesser personnel, and we participated in an

DOCID: 3189576

advisory capacity to the FA.

I may loyally affirm that the workers of the FA collaborated with us openly and honorably, withheld nothing from us, and this furthered our work. In spite of good results which the FA finally reached in the course of its 11 years of existence, it was not able to furnish proof of its right to existence. But this proof was never required of it.

CHAPTER VIII. SOME CRYPTANALYSTS IN THE FOREIGN OFFICE

Preliminary remarks: In the course of many years work with many cryptanalysts I have learned to distinguish two different types among them: one type with linguistic knowledge and proficiency but without particular inclination for work on purely technical cryptanalytic problems such as reenciphorments etc., and another type with mathematical ability and knowledge, without particular inclination for the linguistic tasks of decipherment. Each of these types inclines more or less to over-evaluation of his own part of the work and to underestimation of the efforts of the other type. I know a few cryptanalysts who are gifted more or less equally for both linguistic cryptanalysis (code recovery) and also for purely technical cryptanalytic work. (To these rare cryptanalysts belongs Ministerialrat Dr. Seifert, the Chief of the Austrian Cryptanalytic Service.) I myself, in my work, have been equally concerned with the problem of linguistic cryptanalysis as well as with purely technical cryptanalytic work. I am thus able to look objectively at both types of cryptanalysts from my own knowledge of the special difficulties and demands of their work and their methods, and in the following opinions I have characterized the persons concerned without any prejudice.

(a) Dr. Hans BENZING is an extraordinarily gifted linguist and a distinguished expert in the Turkish language, the languages of the Turkish people, and in other Near Eastern tongues. In cryptanalytic technique he has worked only in the field of relatively simple Turkish ciphers; yet he is skilled in these. He has solved a large number of codes independently and with scientific precision. He is energetic and methodical, an amiable fellow worker, colleague, and superior. A good

career as linguist should await him.

(b) WILHELM BRANDIS is a reliable, hard working civil servant, and a competent expert in French, Swiss, and Belgian codes, some of which he has independently solved. In cryptanalytic technique he always stood in the shadow of his personal friend, Dr. H. KUNZE, with whom he has worked for many years and to whose authority in this field he willingly subordinated himself.

(c) Dr. HELMUT GRUNSKY is an extraordinarily competent mathematician who worked successfully during the war in the field of cryptanalytic technique and completed various difficult mathematical investigations and calculations. He is the quiet and modest scholarly type.

(d) Miss URSULA HAGEN is among the best and most successful cryptanalysts who have worked in the Foreign Office. She is a highly talented and painstaking solver of codes and writes with this an outright gift for technical cryptanalytic work. She has independently solved a great number of codes and reciphernents. She worked in a particularly broad field in which she was able to use her outstanding knowledge of the English, Spanish, and Portuguese languages. She possesses great organizing powers and is complete master of the art of handling personnel. Highly trained, cultivated, and amiable, she was dearly loved and treasured superior, colleague, and associate.

(e) ERNEST HOFFMANN proved himself in the First World War a successful cryptanalyst of English military cipher systems. In the Foreign Office he worked with great skill and good results linguistically on code and also as a cryptanalytic technician. He is an intelligent, skilled, energetic, and ambitious man. Since about 1936 he has no longer worked in cryptanalysis but carried out technical communication assignments.

(f) Dr. PAUL KASPER chiefly concerned himself with Roumanian codes of which he has solved a number. In spite of his intelligence, his keen intellect, and his wit he lacked the vivacity of mind essential for technical cryptanalysis. His slowness and a certain lack of initiative hampered his work.

(g) Dr. ERNST KUNZE is one of the most competent and productive cryptanalysts of Germany. He has carried through a large number of difficult cryptanalytic problems or has furthered them through advice. He possesses a special faculty of seeing a problem clearly and simply and of developing and employing effective methods for its solution. He inclines to underestimate linguistic cryptanalysis with which he had very little concern and with more difficulties and presuppositions he is not sufficiently familiar. Since in addition he possesses a very high self-esteem and cannot compromise, he was often very difficult as a fellow-worker and colleague. I myself, however, have worked with him gladly and with good results for us both; yet I was probably the only one of his colleagues whom he accepted at full value.

(h) Dr. BRUNO LEHMANN is very gifted linguistically and is master of a number of languages. He worked chiefly on Greek codes. In spite of linguistic ability he lacked the combinatory faculty necessary for linguistic cryptanalysis and the necessary knowledge of political affairs. Therefore, his success in his work was small. He had almost no work in cryptanalytic technique.

(i) Dr. HANSKURT MUELLER is scientifically well-trained and an expert in the English and the Scandinavian languages. He is a first-rate translator. He worked successfully on the solution of some American codes and proved himself superior. Also in the solution of the American strip systems, after the successful completion of the technical crypt-analysis, he completed the linguistic cryptanalysis with great skill. He had very little occasion to concern himself with cryptanalytic technical work yet he was skilled in this also. After the transfer of Mr. ZASTROW to OKW/Chi he was made head of the American desk in the Foreign Office. He is a quiet, modest man of blameless character, but he is slightly hampered by nervousness.

(j) Dr. PETER OLBRICHT is an important, scientifically trained student of Japanese and Chinese language and custom who, as chief co-worker of Mr. SCHAUFFLER, worked successfully in the linguistic, and to a lesser degree in the cryptanalytic technical field - but here too with

skill. An intelligent, highly educated man.

(k) Prof. DR. HANS FORBACK can be designated as the most capable and most productive cryptanalyst in the technical cryptanalytic field of the war workers of the Foreign Office. He is a first-rate mathematician who combines his significant theoretical knowledge with a highly practical sense for its application to cryptanalysis. He has brilliantly carried out many difficult cryptanalytic problems with great skill, among others the solution of Chinese permutations. His calm, amiable, trustworthy, and at the same time modest nature as well as his worldly wisdom made him a very esteemed colleague and co-worker.

(l) RUDOLF SCHAUFFLER is that rare combination of gifted mathematician and capetent linguistic expert. He has acquired in his work complete mastery of the Japanese language and is properly hailed as the greatest expert on Japanese telegraphic texts in Germany. He has solved most Japanese cryptographic systems linguistically, but partly also by cryptanalytic technique. He is full master of the difficult art of translating Japanese texts. In the field of purely technical cryptanalysis he was surpassed by many colleagues and fellow-workers; however, he is a brilliant systematizer who systematized all solved cipher systems, and formulated scientifically their presentation and the methods employed, and strove for the development of correct terminology. As a highly able and modest, though slight supercilious man of blameless character he enjoyed universal esteem.

(m) HERMANN SCHEERSCHMIDT is a scientifically trained philologist who has successfully adapted the exact methods of philology to cryptanalysis. He knows well the Slavic and Turkish languages and has solved many codes in various languages. The exactness of his methods which many times crossed the border of pedantry without however encroaching upon the vivacity of his spirit, he has passed on to a number of his younger co-workers (for example: Dr. BENZING) and in this manner has trained them as successful cryptanalysts. He also has an understanding of technical cryptanalytic problems in which he has worked in the Polish and Yugoslav fields - at least in associ[illegible]

DOCID: 3189576

with technical cryptanalytic experts.

(n) KURT SELCHOW headed the Cipher Section of the Foreign Office from 1939-1945. He never was and never will be an expert in this field. He was primarily the organizer and manager of cryptographic matters in the Foreign Office. In this capacity he was a skilled technician in negotiation and consequently he had very little to do with the organization of his own section. He allowed his professionally trained associates a high degree of independence, by which means he obtained their very best efforts. His knowledge of people, both of which he made very great, enabled him to [illegible] by his activity.

(o) KARL PASTRON is a gifted cryptanalyst in the linguistic and cryptanalytic technical fields. He has solved various systems and ranks as an expert in three countries and in American fields. He could have accomplished important things if he had not been interrupted from purposeful and energetic efforts by his apathy and [illegible] which increased as time went on